U.S. Department of Justice

United States Attorney
Eastern District of New York

610 Federal Plaza
Central Islip, New York 11722

ALB:CPK:BTR
F. #2016R01831

June 21, 2019

By ECF

The Honorable Joan M. Azrack
United States District Judge
United States District Court
920 Federal Plaza
Central Islip, New York 11722

Re: United States v. Enayatullah Khwaja , et al
Docket No. 18-CR-607 (JMA)

United States v. Mahmoud Ali Barakat, et al
Docket No. 18-CR-292 (S-1)(JMA)

Dear Judge Azrack:

The government respectfully submits this letter in response to the second of six Court Orders issued from the bench on June 13, 2019 at a conference in the above-referenced cases. All six Court Orders directed the Government to take specified action by a date certain. The second Order directed the government to file a letter by June 21, 2019 setting forth the (i) the government's position regarding bulk cell phones seized at the execution of the search warrant at 500 Smith Street, Farmingdale, New York and (ii) the status of destroying/deleting/returning seized items not within the scope of the search warrants. This letter also responds to the letter of June 17, 2019 from defendants Abdulrahman Khwaja and Shikeba Rhamatzada ("Defendants' June 17, 2019 Letter") which, apart from the ad hominem attacks, stated falsely that (i) the government failed to provide a search protocol and (ii) the government needed to state when the bulk cell phones and a bank account will be returned.

A. As the Chart Indicates, the Bulk Cell Phones Are Available for Pickup

As to the bulk cell phones seized from 500 Smith Street, those phones have been photographed and are available for pickup through arrangements with Customs and Border Protection (CBP). CBP will be contacting the defense attorney to arrange pickup.

The chronology is that when National Electronics first demanded return of the cell phone inventory, the government declined to return the inventory because it elected to commence a timely administrative forfeiture proceeding. After the administrative forfeiture proceeding concluded upon CBP's receipt of National Electronics' claim to the inventory, the U.S. Attorney's Office decided not to pursue judicial forfeiture of the inventory. Accordingly, after determining that the inventory was fully photographed and no further action was needed to preserve that evidence for trial, the government made the cell phone inventory available for pickup by National Electronics, as reflected in the chart attached to the June 14th letter of the Government and as conveyed to National Electronics' counsel. Defendants' claim that the chart attached to the Government's June 14, 2019 letter is inaccurate because it states the bulk cell phones are available for pickup is untrue, in fact, as the bulk cell phones are available for pickup.

Regarding the bank account, Counsels' assertion that the government is "now searching" for the Taban Company Habib Bank Account funds is not true. In fact, before Defendants' June 17, 2019 Letter, during a conversation with Mr. Riopelle on Friday, June 14, 2019, the Acting Director of FP&F at JFK Airport, stated, in sum and substance, that the return of the funds by ACH would take approximately one week from the time defense counsel returns the ACH form to FP&F for processing. Indeed, defense counsel provided his attorney trust account information for purposes of receiving the funds. Thus, the timing of the return of the funds depends upon the normal factors that govern these situations, i.e., receipt of properly executed ACH forms and normal bank transaction time periods, rather than the government's "searching" for the funds, as defense counsel inaccurately states.

B. Destroying Irrelevant Portions of the Image of the Computer Before Trial Would Destroy Its Evidentiary Value and Is Not Required By the Law

The government has searched the hard copy documents seized and returned those found to be irrelevant. As to the electronics data, the Government intends to retain the images made of electronic devices containing evidence for trial until the conclusion of this case. To destroy portions of the images created would destroy the admissibility of the evidence. As set forth below, the law does not require the Government to destroy irrelevant portions of seized electronic evidence prior to the conclusion of the criminal case. Courts recognize the reality that "it may be necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for purposes of trial." In the Matter of a Warrant for All Content and Other Information Associated with the Email Account, 33 F.Supp.3d 386 (S.D.N.Y. 2014) ("Google Case") (noting that "while Ganias expressed skepticism about the need for retaining non-responsive files for this purpose, it was willing to 'assume' the need existed and stated that in such an event, the retained material should not be used 'for any other purpose' – presumably referring to the material's use in that case as the basis for a second warrant."). Here, the Government is only searching the electronic evidence in connection with this prosecution. Defendant's citation of the irrelevant Metter and Debbi cases does not aid their demands. Metter dealt with a case in which the Government did not begin its review for 15 months after seizure. Here, the review started on the day of seizure. As for the Debbi case, that

deals with both the failure to separate out personal files from responsive ones during searches of residences and the failure to begin review of seized evidence, there seven boxes of material that "plainly fell outside" the proper parameters. Neither situation is present here.

Images were made on the day of the search of dozens of computers. Defense counsel seeks the date when the Government will be destroying the irrelevant portions of the electronic evidence seized.

The process of searching the seized electronic evidence started on the day of the execution of the search warrant. The process differs for certain items. As to the thumb drives and hard drives, the device was hooked up to writeblocker and a forensic image was created. Next, a forensic agent can put the forensic image into forensic software. These two steps make the hard drive or thumb drive searchable. Depending on the size of the content (megabytes v. terabytes) of the device, these steps can take from forty minutes to days where the device has many terabytes of information. The hard drive on a typical computer takes one agent two days from hooking the device up to write blocker software to turning the searchable forensic image over to the searching agent. Although the standard practice is to have one person create the searchable forensic images because that person will be a witness at trial, that was not the practice followed here over the past seven months. Due to the volume of devices seized, from the day of the execution of the search warrant, the government has had multiple forensic agents perform this task. Generally, agents cannot deal with anything except an image for their search purposes. There are, of course, rare instances where an image cannot be created and, typically, the device is returned. In this case, as the chart attached to the June 14th letter evidences, many devices on which images were not able to be created were returned.

In terms of deleting/destroying irrelevant material on an electronic device with trial evidence on it, that is not the generally accepted practice. If an image is to retain its evidentiary value, it must retain the hash value it had at its creation. A hash value, like a fingerprint, identifies the image. Deleting anything from the image will tamper with the hash value and, consequently, its admissibility at trial. If an image is to retain its evidentiary value, no part of the image may be deleted.

As to cell phones, unlike thumb drives and hard drives, they must be turned on for extraction because there is no hard drive to image as cell phones consist, in their core, of memory chips on a board. Here, with the cell phones, starting at the time of the search, first, the device was hooked up to Cellebrite software. Then, using the Cellebrite software, a forensic agent conducted extractions of data from the applications on the phone including, for example, text messages, whats app communications and photographs.

C. Since the Day of the Search, the Government Has Been Searching Seized Devices

Defendants' June 17, 2019 Letter further claims inaccurately that the government "has not conducted any search whatsoever" of the nearly 400 devices and documents it seized seven months ago (page 1). This statement is also false. Their letter further claims falsely that, in seven months, the government has done "nothing" (Page 1).

The truth, not found in Defendants' June 17, 2019 Letter, is that, in seven months, the Government, has had many agents working on searching evidence in this case. Certainly, as the exhibit to Government's June 14th letter evidences, a group of devices were analyzed and returned as "not being used for evidence." In another category, including about a dozen devices, attempts to image a device were unsuccessful and those devices were returned.

Contrary to the defendants' claims that no searches have been done, using a team of approximately eight full time agents including forensic agents, the government has been searching cell phones, hard drives, thumb drives and computers, including materials on the eight terabytes of data recently produced, since the day of the search. Commencing Monday June 24, 2019, although more agents have been requested, due to emergencies, arrests and searches, it is expected that there will be approximately eighteen full team agents engaged in searching forensic images that have been created by forensic agents of seized devices.

As referenced in the Government's June 14th letter, the process of searching the two servers is significantly different from searching all the other electronic devices. The servers can have 40-50 work stations working off them and the complexity of searching them arises, in part, from that fact. On the day of the search, no image was able to be made of the two servers electronically. Therefore, on site, because the government was working to minimize disruption, an extraction of the servers was done using backup software. Thereafter, the government had to obtain software to create a visualized server. That is the procedure referenced in the June 14th letter and is ongoing. The two servers are the items on which searchable databases have not yet been created.

D. The Government Supplied its Search Protocol

In response to Defendants' June 17, 2019 Letter, the claim that the government failed to supply its search protocol is false as it was provided in the June 14th letter. Defendants' letter states, in italics, that the government "has no search protocol" (page 1) when, in fact, the government supplied the search protocol it has been using in searching imaged computers including their hard drives. Defendants' letter simply makes up this conclusion and claims the government's letter states that when it does not. Unsurprisingly, Defendants' letter fails to cite any part of the June 14th Letter for this inaccurate conclusion.

As stated in the Government's June 14th letter, the search protocol for hard drives, thumb drives and computers has been:

Once items are placed in searchable formats, the search protocols proceed from the language and limitations of the search warrant. Specifically, first a search is done by date to limit the universe to dates within the chronological parameters of the search warrants creating the time relevant subset. Second, using the time relevant subset, a search of names, both individuals and businesses, is done to obtain all documents within the relevant time period that mention either a company or individual identified in the search warrant whose records are within the scope of the search warrant. The time relevant subset is also searched for English and Spanish words that are believed from an investigative point of view, to be relevant. For example, words relating to the crimes identified in the search warrants (e.g., cash, dinero, money, invoices, statements) have been used as a subset to search the time relevant subset. Subsequently, additional searches are conducted using search terms based upon the contents of retrieved relevant documents and information being continuously received from individuals with knowledge of defendants' money laundering operations.

This search protocol will change and has been evolving since the devices were imaged. Search protocols, of necessity, evolve during searches due to misspellings and terms and codes learned from proffers, informants and examination of the electronic device itself. As the United States Court of Appeals for the Second Circuit stated: "Even simple codes can defeat a pre-planned word search." United States v.Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017)

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

By: /s/
Charles P. Kelly
Burton T. Ryan
Assistant U.S. Attorneys
(631) 715-7866

cc: All Defense Counsel
(via ECF and E-Mail)